Case study

Poached payment

Fraudster impersonates an insurance brokerage to siphon off customer payment

Funds transfer fraud - whereby fraudsters dupe innocent businesses and individuals into transferring what they believe are legitimate payments to fraudulent bank accounts - is becoming an increasingly common problem.

In an insurance context, most cyber policies with crime cover in place will provide some form of protection for situations where policyholders lose their own money in this way. For example, if a fraudster manages to impersonate the policyholder's CEO and gets a member of the finance team to send a payment over to a fraudulent bank account, the policyholder's business will have suffered a financial loss. All being well, this loss can then be recovered under their cyber policy.

However, it's not always the policyholder's business that suffers a loss in this way, but the policyholder's customers. Customer payment fraud describes a situation in which a business is impersonated by a fraudster, who then dupes some of the business's customers into making payments to a fraudulent account.

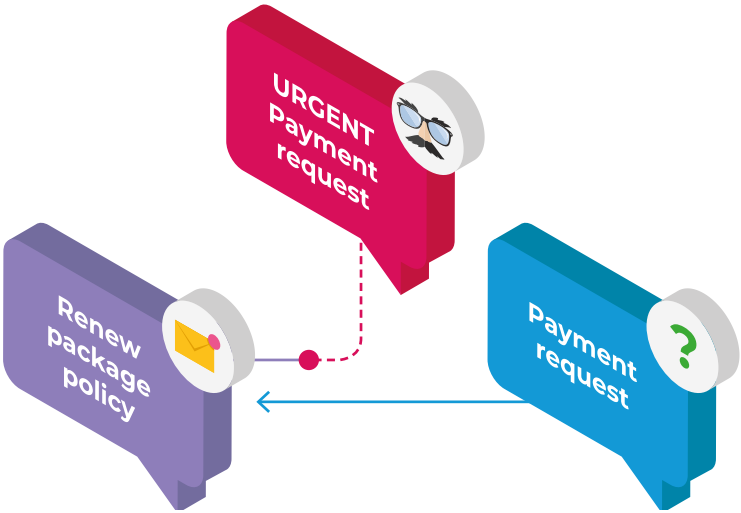
One of our policyholder's affected by such a loss was a small insurance brokerage that is primarily involved in arranging property and casualty insurance cover for small and medium-sized businesses.

Phishing scam opens gateway to broker's email account

The scam all began when one of the brokerage's employees received an email from what appeared to be one of his trusted contacts. The email stated that this trusted contact had used a document sharing platform to upload some important documents for this broker to view, attaching a link to enable the broker to review the documents. Upon clicking on the link, it took the broker onto a seemingly legitimate landing page and explained that he could view the documents by using his email login. Believing that this was a genuine attempt to share some documents, the employee decided to input his email login details. By inputting these details, however, **the broker was unwittingly handing over his email login credentials** to a fraudster.

With these credentials now at his or her disposal, the fraudster was able to browse the broker's inbox and identify any opportunities to intercept payments. As it happened, the broker had recently been working on the renewal of a package policy for one of the brokerage's existing clients. After some negotiation, the client had agreed to renew the policy with their current insurer at a premium of $14,580. The client had **opted to pay in one lump sum** as opposed to instalments and so the only thing left to do was for the client to transfer over the funds for the premium to the brokerage, who would then send these funds over to the insurer. The most recent communication between the broker and the client had involved the broker sending over account details and the client responding to explain that they would look to send over the funds in the next five working days.

Having spotted an opening, the fraudster chose this moment to act. Prior to contacting the client, the fraudster's first move was to put a forwarding rule in place on the broker's email account. Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within a certain criteria are automatically forwarded either to a specific folder or another email account. To help reduce the risk of the scam being uncovered, in this instance the fraudster set up a forwarding rule that meant that any **incoming email that came from an account with a domain name that matched that of the broker's client** would automatically be marked as read and sent to a pre-existing, but largely neglected folder within the broker's email account entitled "RSS Feeds".



Client tricked into sending premium to fraudulent account

Now that this forwarding rule was in place, the fraudster logged into the broker's email account and sent an email to the client. The email stated that due to an ongoing audit, the insurance brokerage couldn't receive payments into their usual account, but went on to explain that in the meantime payments could be made into the brokerage's international account, with the fraudster providing the new wiring instructions in an attachment. To **add a sense of urgency,** the fraudster also mentioned that the insurer had been chasing up payment of the premium and so requested that the client make the payment into the international account as soon as possible.

As the email had come from the broker's genuine email account and provided a seemingly plausible reason for the change of account, the client assumed that this was a legitimate request and so they duly sent over the funds on the same day. The client also responded to the broker's email later that day to confirm that they had sent over the funds to the international account and that the brokerage could expect to receive them in a few days' time. To make sure that the payment had

been processed, the client asked for a confirmation from the broker when the funds had been received. As the forwarding rule was in place, however, only the fraudster could see this email, and to allay any concerns that the client might have if they didn't hear back from the broker, **the fraudster impersonated the broker again a few days later** and confirmed that the funds had been received.

With the client believing that they had paid the premium and that the funds had been received by the brokerage, they gave no further thought to the matter until the broker sent over a genuine email some weeks later requesting an update on the payment. The client picked up the phone to query this and explained that they had already paid, and it was only at this point that the scam was uncovered. The incident was reported to local law enforcement and all of the banks involved in the transaction were informed, but the premium had been transferred to an account in Hong Kong and all of the funds had been emptied from the account by the time that the fraud was discovered.

With the funds deemed unrecoverable, the client still had an outstanding premium payment to make. However, because the email with the fraudulent instructions had come from the broker's genuine email account, the client argued that it was not their fault that the funds had been misdirected and instead put the blame on the brokerage for having had their computer systems compromised and misused by the fraudster. Given this, the brokerage accepted responsibility for the incident and decided to pay their client's premium from their own funds. They were then able to recoup this loss under the cybercrime section of their cyber policy with CFC, which provides cover for customer payment fraud up to a maximum of $50,000.

The brokerage accepted responsibility for the incident and decided to pay their client's premium from their own funds. They were then able to recoup this loss under the cybercrime section of their cyber policy with CFC

Even customer losses can end up costing businesses dearly

This claim highlights a few key points. Firstly, it shows **just how canny cybercriminals are becoming at parting individuals and businesses from their money**. In this case, the fraudster managed to successfully impersonate one of the broker's trusted contacts and lured the broker into volunteering his email login details; took their time to find a suitable customer to target; set up a forwarding rule to prevent the broker from coming across any email responses from the client relating to the scam; came up with a credible reason as to why the client would need to send over the funds to a different account; encouraged the client to pay quickly by explaining that the insurer was chasing up the premium; as well as confirming to the client that the payment had been received to avoid any further questions or concerns from the client if they didn't hear back.

Secondly, it illustrates an interesting dynamic between businesses and their customers. When a business is impersonated by a fraudster who manages to trick a customer into transferring funds to a fraudulent account, **many customers will place the blame on the business** that was impersonated and seek reimbursement for their loss, especially if it was the business's systems that were compromised and used to facilitate the fraudulent communications.

Finally, it highlights the need for customer payment fraud cover in cyber policies. Many cyber policies with crime sections will only provide cover for losses that directly affect an insured. But in this case, **it wasn't the insured that suffered a direct loss but their customer**. However, because the customer blamed the insured for their loss, the insured were under pressure to reimburse the client. With more and more financial transactions being carried out electronically and with more and more cybercriminals looking to intercept them, the chances of a business's customers falling for a scam of this nature are only increasing and it's usually the business that's been impersonated that will take the blame. That's why it's a good idea to check your cyber policy for customer payment fraud cover. ●